training code: MS Copilot Sec / ENG DL 1d / EN

Govern and Secure Microsoft 365 Copilot

This instructor-authored course provides a practical, end-to-end overview of how to deploy, administer, and govern Microsoft 365 Copilot and Copilot agents in an enterprise environment. It covers the core architecture and data flow of Copilot—where prompts are grounded in Microsoft Graph data within the Microsoft 365 service boundary—and explains licensing, access, and administrative controls available in the Microsoft 365 admin center.

Participants learn how to configure, test, publish, and manage agents using Copilot Studio and Power Platform tools, including distribution across Teams, Microsoft 365 apps, and web channels.

The training also introduces Microsoft's Responsible AI principles and shows how to apply built-in moderation, safety, and policy controls to guide agent behavior.

Finally, the course covers essential data-security capabilities in Microsoft Purview—sensitivity labels, DLP, Audit, eDiscovery, Insider Risk Management, and Adaptive Protection—as well as monitoring AI usage and securing browser-based interactions with AI apps.

Training recipients

This course is designed for :

- IT administrators,
- security and compliance professionals
- Power Platform makers
- technical decision-makers responsible for deploying, governing, and securing Microsoft 365 Copilot and Copilot agents.

It is also suitable for architects and digital transformation leaders who must understand how Copilot integrates with organizational data, identity, and security frameworks. Participants should have a foundational understanding of Microsoft 365 administration and enterprise security concepts.
The purpose of this training is to equip organizations with the knowledge and practical skills needed to safely and effectively implement Microsoft 365 Copilot and Copilot agents. The course focuses on architecture, administration, agent lifecycle management, responsible AI governance, and enterprise-grade data protection using Microsoft Purview. By completing this training, participants will be able to manage Copilot deployments, enforce safety and compliance policies, and ensure secure, responsible adoption of AI across their environment

Benefits

- Confidence in planning and deploying Microsoft 365 Copilot across the organization
- Ability to create, publish, and manage Copilot Studio agents effectively
- Practical understanding of Responsible AI and content-moderation controls
- Enhanced data protection through Microsoft Purview (DLP, sensitivity labels, IRM, Audit, eDiscovery)
- Awareness of AI-related risks and the ability to monitor them using DSPM and Microsoft Edge for Business protections
- Preparation for secure, scalable AI adoption in enterprise environments.

This training gives you clear, practical confidence in deploying Microsoft 365 Copilot by explaining how its architecture, data access, permissions, and licensing work in real organizational environments. You also gain the ability to independently create, test, publish, and manage Copilot Studio agents, enabling you to deliver meaningful automation and assistance without external support. The course strengthens your understanding of Responsible AI, helping you set moderation levels, control sensitive topics, and guide agent behavior safely and consistently. In addition, you learn how to protect organizational data using Microsoft Purview tools such as sensitivity labels, DLP, auditing, and insider-risk controls. Finally, you develop the skills to identify and monitor AI-related risks with DSPM and Microsoft Edge for Business protections, ensuring secure, compliant, and well-governed AI adoption across your organization

Training program

1: Foundational Administration and Deployment

- Introduction to Copilot Architecture
  Understand the capabilities, architecture, and licensing models of Microsoft 365 Copilot and its agents.
- Administrative Setup
  Manage licenses and access controls using the Microsoft 365 Admin Center.

- Deployment and Adoption
  Develop deployment strategies, explore practical use cases, and monitor billing and usage to drive organizational adoption.
- Prompt Governance
  Implement administrative tasks to oversee prompt management within the organization.

2: Agent Management

- Agent Configuration
  Configure user access and permissions; create, edit, and test Copilot agents.
- Lifecycle and Environment Management
  Monitor agent lifecycle using Power Platform tools; manage environments, including importing and exporting agents.
- Publishing and Distribution
  Distribute agents across Microsoft Teams, custom websites, and mobile apps.

3: AI Governance and Content Moderation

- Responsible AI Principles
  Align administration with Microsoft's AI principles: transparency, accountability, fairness, and safety.
- Moderation Mechanisms
  Configure content moderation levels (High, Medium, Low) to block or modify agent responses based on safety policies.
- Instructional Control
  Use agent instructions to restrict topic scope, manage "no-go" areas, and customize fallback behaviors.
- Runtime Security
  Verify authentication requirements and monitor runtime protection for deployed agents.

4: Securing Data with Microsoft Purview

- Information Protection
  Apply sensitivity labels and Data Loss Prevention (DLP) policies to ensure AI respects data protections.
- Data Security Posture Management (DSPM)
  Discover AI-related risks and identify AI tools in use across the organization.
- Compliance and Auditing
  Use Audit for visibility into prompts and responses; apply eDiscovery for compliance investigations.
- Risk Mitigation
  Implement Insider Risk Management and Adaptive Protection to prevent oversharing of sensitive data

Expected preparation of the participant

- Basic understanding of Microsoft 365 services
  - Participants should know how core services such as SharePoint, OneDrive, Teams, and Exchange

function within the organization.

- Familiarity with Microsoft 365 administration concepts
  - A general awareness of admin roles, permissions, and tenant-level configuration is recommended.
- Foundational knowledge of security and compliance principles
  - Helpful for understanding how sensitivity labels, DLP, auditing, and governance policies interact with Copilot and Purview.
- Experience with cloud-based enterprise tools
  - Participants should feel comfortable navigating web-based admin portals and cloud management interfaces.
- Basic familiarity with Microsoft 365 Copilot features
  - Participants should understand what Copilot is, how prompts work, and where Copilot appears in Microsoft 365 apps—so the training can build on that foundation rather than introduce Copilot from scratch.

To increase the comfort of work and training's effectiveness we suggest using an additional monitor. The lack of additional monitor does not exclude participation in the training, however, it significantly influences the comfort of work during classes.

You can find information and requirements of participation in Distance Learning trainings at: https://www.altkomakademia.pl/en/how-it-works/about-courses/

Training Includes

- manual in electronic form available on the platform: https://www.altkomakademia.pl/
- access to Altkom Akademia's student portal

Training method:

- Lecture (20%)
- Workshops (20%)
- Exercises (60%)

Duration

1 days / 7 hours

Language

- Training: English
- Materials: English